UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,157	10/20/2003	Andrew M. Spencer	10013891-1	9457

22879 7590 06/15/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
06/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/689,157
Filing Date: October 20, 2003
Appellant(s): SPENCER, ANDREW M.

Mr. Steven L. Nichols
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 29, 2010 appealing from the Office action mailed November 27, 2009

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

A list of claims that included in the appeal brief filed on March 29, 2010 is incorrect. The corrected list of claims is addressed below.

The following is a list of claims that are rejected and pending in the application:

1. Claims 1-30 are pending
2. Claims 1-15, 28 and 29 are rejected
3. Claims 16-26 are withdrawn
4. Claims 27, 30 are cancelled

Based on the after final that has been filed in by the appellant on September 15, 2008, this amendment After-Final has been entered (see, date filed 10/1/2008, Amendment After Final or under 37CFR 1.312, initialed by the examiner for "OK TO ENTER" and dated 09/25/2008). Therefore, claims 27 and 30 current status should be cancelled. In addition, the appellant appears to ignore or overlook the advisory action mailed out 10/1/2008 with response to the arguments about the amended limitation filed

09/15/2008 from amendment after-final, in which the examiner considered the amended limitation of claim 28, which has been amended to incorporate the elements of claim 30 (now is cancelled). And thereafter, all the office actions that examiner mailed out after that amendment after-final filed 9/15/2008, have been consistently addressed that claims 27 and 30 are cancelled.

(4) Status of Amendments After Final

There is no Amendment After Final before the appeal brief that file on March 29, 2010.

(5) Summary of Claimed Subject Matter

The Summary of Claimed Subject Matter is appeared to be, once again, incorrect.

As per claim 27, according to the list of claims above that listed in (3) Status of Claims, claim 27 that mentioned on page 7 of the appeal brief filed on 3/29/2010, is moot and should not be included with this brief, since claim 27 is cancelled.

As per claim 28, the appellant did not include the limitation that was incorporated from claim 30 based on the amendment after final filed on 9/15/2008. The current status of claim 28 should be read as follows:

28. A method of decrypting encryption keys in an information storage device, comprising:

reading the encrypted encryption keys from a magnetic random access memory;

reading a master encryption key from a first non-volatile memory;

decrypting each one of the encryption keys using the master encryption key;

encrypting data using the encryption keys; and

writing the encrypted data to the magnetic random access memory.

For the above reasons, examiner believes that there should only be two independent claims to be addressed in this summary of claimed subject matter, which is claims 1 and 28.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The Claims Appendix is appeared to be, once again, incorrect.

As per claim 27, according to the list of claims above that listed in (3) Status of Claims, claim 27 that mentioned on page 7 of the appeal brief filed on 3/29/2010, is moot and should not be included with this brief, since claim 27 is cancelled.

As per claim 28, the appellant did not include the limitation that was incorporated from claim 30 based on the amendment after final filed on 9/15/2008. The current status of claim 28 should be read as follows:

28. A method of decrypting encryption keys in an information storage device, comprising:

reading the encrypted encryption keys from a magnetic random access memory;

reading a master encryption key from a first non-volatile memory;

decrypting each one of the encryption keys using the master encryption key;

encrypting data using the encryption keys; and

writing the encrypted data to the magnetic random access memory.

As per claim 30, according to the list of claims above that listed in (3) Status of Claims, claim 30 that mentioned on page 31 of the appeal brief filed on 3/29/2010, is moot and should be cancelled.

(8) Evidence Relied Upon

5,159,182	Eisele	10-1992

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Eisele (US 5,159,182).

a. *Referring to claim 1:*

i. Eisele teaches a removable information storage device (see Figures 2 and 3) suitable for use with a host, comprising:

(1) a non-volatile memory (e.g. memory 9) configured to store a master encryption key **(see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele)**; and

(2) a non-volatile magnetic memory configured to store encryption keys which have been encrypted using the master encryption key and to store data which has been encrypted using the encryption keys **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele)**.

3. Claims 2-15, 28-29 are rejected under 35 U.S.C. 102(b) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Eisele (US 5,159,182).

a. *Referring to claim 28:*

i. Eisele teaches a method of encrypting encryption keys using a master encryption key in an information storage device, comprising:

(1) reading encrypted encryption keys from a magnetic random access memory; reading a master encryption key from a non-volatile memory **(see Figures 5-6; and column 5, lines 5-9 of Eisele)**;

(2) decrypting each one of the encryption keys using the master encryption key **(column 5, lines 12-19 of Eisele)**;

(3) encrypting data using the encryption keys **(column 5, lines 12-19 of Eisele)**; and

(4) writing (e. g., storing) the encrypted data to the magnetic random access memory **(see Figures 2-3 and column 5, lines 12-24 of Eisele)**.

ii. Although Eisele teaches the claimed subject matter, Eisele does not clearly use the term “magnetic random access memory (MRAM)“ for disk 7 as

shown in Figure 3. However, Eisele implies that the magnetic disk includes read/write heads 16 and 17, wherein MRAM uses the same read/write functionality as in disk 7 of Eisele.

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have modified the invention of Eisele to clearly disclose disk 7 as being a magnetic random access memory (MRAM) **(see Figure 3).**

iv. The ordinary skilled person would have been motivated to:

(1) have modified the invention of Eisele to clearly name the removable storage device disk 7 as any different type of programmable memory or storage device to store encryption keys, master keys, encryption/decryption data, program, etc.

b. *Referring to claim 29:*

i. Eisele further teaches:

(1) reading encrypted data from the magnetic random access memory **(see Figures 5-6; and column 5, lines 5-9 of Eisele)**; and

(2) decrypting the encrypted data using the encryption keys **(column 5, lines 12-19 of Eisele)**.

c. *Referring to claim 2:*

i. Eisele further teaches:

(1) an encryption and decryption engine configured to encrypt and decrypt the encryption keys using the master encryption key and to encrypt and decrypt the data using one or more of the encryption keys **(column 5, lines 12-19 of Eisele).**

d. *Referring to claim 3:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a magnetic memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

e. *Referring to claim 4:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a read-only memory which includes fuse elements **(see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele).**

f. *Referring to claim 5:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a nitrided read-only memory **(see Figures 2, 3, and 8, element 9; column 4, lines 6 and 40; and column 5, lines 20-24 of Eisele).**

g. *Referring to claim 6:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is an erasable programmable read-only memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

h. *Referring to claim 7:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is an electronically erasable programmable read-only memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

i. *Referring to claim 8:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a flash erasable programmable read-only memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

k. *Referring to claim 9:*

i. Eisele further teaches:

(1) wherein the first non-volatile memory is a one time programmable read-only memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

l. *Referring to claim 10:*

i. Eisele further teaches:

(1) wherein the non-volatile magnetic memory is a magnetic random access memory **(see Figure 3, element 7; column 4, lines 18-28; and column 5, lines 20-24 of Eisele).**

m. *Referring to claim 11:*

i. Eisele further teaches:

(1) wherein the second non-volatile memory is partitioned into first and second areas, and wherein the encrypted encryption keys are stored in the first areas and the encrypted data is stored in the second areas **(column 5, lines 20-30 of Eisele).**

n. *Referring to claims 12-13:*

i. These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

o. *Referring to claim 14:*

i. Eisele further teaches:

(1) wherein the first areas are located at one or more predetermined address locations within the second non-volatile memory **(column 5, lines 20-30 of Eisele).**

p. *Referring to claim 15:*

i. Eisele further teaches:

(1) wherein the first areas are located at one or more random address locations within the second non-volatile memory **(column 5, lines 20-30 of Eisele).**

(10) Response to Argument

I. Applicant has argued that Eisele does not teach or suggest a storage device having "a non-volatile magnetic memory configured to store encryption keys which have been encrypted using a master encryption key," *where the "master encryption key" is stored on a separate "non-volatile memory" of the storage device*, as cited in claim 1 (see first paragraph, page 11 of appeal brief).

Examiner respectfully disagrees with the applicant and still maintains that:

First of all, Eisele does teach the claimed subject matter. It is clearly in Figure 2, 3, and 8, element 9 is a memory and column 5, lines 20-24 of Eisele stated that in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. (e.g., encryption key or master encryption key, etc..) in such a way that they cannot be reproduced. Figure 3 of Eisele clearly discloses element 9 is non-volatile memory and disk 7 is non-volatile magnetic memory. Therefore, Eisele precisely teaches the use of the two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claim 1.

Secondly, appellant re-paraphrased the above language that does not even recite in the original claim 1, which could construe new matter. Specially, appellant stated the language "*where the "master encryption key" is stored on a separate "non-volatile memory" of the storage device,* when the evident on page 25 of appeal brief, under the section of claims appendix, showing claim 1 did not recite,

include or even mention the master encryption key is stored on **a separate non-volatile memory of the storage device** *(emphasis added)*.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *where the "master encryption key" is stored on a separate "non-volatile memory" of the storage device*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

II. Appellant also argues that Eisele does not teach or suggest the use of different types of encryption keys, or that one type of encryption key is used to encrypt encryption keys of a different type, as cited in claim 1. Even if, arguendo, Eisele did teach or suggest the "master encryption key" and other "encryption keys" recited in claim 1, where the master encryption key is used to encrypt the other encryption key, the Action has still failed to demonstrate that Eisele teaches storing the master encryption key on one of the storage media and the other encryption keys on the other of the storage media in the same device (see first and second paragraphs, page 12 of the appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

As mentioned above in section (I), Eisele does teach the claimed subject matter. Figure 3 of Eisele clearly shows element 9 is non-volatile memory and disk 7 is non-volatile magnetic memory (emphasis added). More in details, the diskette 7 has

shown in Figure 3 differs from its counterpart in Figure 2 in that it includes a magnetic-disk 15 (i.e., another non-volatile magnetic memory) and has read/write heads 16 & 17 of known design instead of the magnetic-interface 6 of Figure 2. Therefore, Eisele precisely teaches the use of the two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys in the same device, as recited by claims 1. From a technical point of view, it is a very common standard in the art that a memory and/or a storage media can configure to store not only encryption keys or master encryption key, but it also can hold/store any kind of content without power being applied. It may refer to chips that are not changeable, such as ROMs and PROMs, or to chips that can be rewritten many times such as flash memory, or disk 15 and 7 as disclosed by Eisele. Being able to hold instructions, data and/or keys without power is essential in a myriad of devices because AC power can fail and batteries become depleted. Again, as mentioned in section (I) above, column 5, lines 20-24 of Eisele stated that in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. (e.g., encryption key or master encryption key, etc..) in such a way that they cannot be reproduced. Therefore, Eisele clearly anticipates each and every element recited in claim 1.

III. Appellant has argued that Eisele has failed to demonstrate “an encryption and decryption engine configure to encrypt and decrypt the encryption keys using the master encryption key (see first paragraph, page 15 of appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

Eisele does teach the limitation as cited in claim 2. In fact, Eisele discloses that It is of particular advantage also to be able **to use processor 2 in the various elements to encrypt and decrypt data by transmitting plaintext data to processor 2 through the interface and back in encrypted form through this interface**. For example, message authentication codes and digital signatures based on RSA-algorthm can be generated and verified as well as digital envelopes can be sealed and opened. In order to use **any of the elements as an encryption/decryption machine** *(emphasis added),* it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. in such a way that they cannot be reproduced (column 5, lines 12-24 and Figures 2 and 3 of Eisele). Thus, Eisele teaches the claimed subject matter of claim 2.

IV. Appellant also has argued that Eisele does not teach or suggest a magnetic RAM anywhere, and does not support the examiner's position, as cited in claim 10 (see lines 2-3, page 16 of appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

It is evident to the Examiner that the instant specification disclosed that a MRAM can also be a magnetic memory (see page 5, lines 14-15 of instant specification) , which is the magnetic disk and/or magnetic medium 15 that showed in Figure 3 of Eisele, wherein data is transferred from processor 2 to the central-unit of a related

computer, for example, in such a way that head 16 writes this data onto magnetic-disk 15 using it as an intermediate memory which is then read by the read/write head of the computer's diskette-drive (see column 4, lines 24-28 of Eisele). Furthermore, by the use of a diskette with a magnetic-disk and a cassette with magnetic tape, it is possible to install a read/write head inside the diskette/cassette. This enables the magnetic medium (tape or disk) to be used as an intermediate storage-facility in that data supplied by the processor is initially recorded on the medium and then read by the read/write head of the EDP-equipment. Obviously it is also possible for data to be transferred in the opposit direction, i.e., recording of data by the read/write head of the EDP-equipment on the medium and the subsequent reading of this data by the read/write head in the diskette or cassette. (see column 3, lines 5-16 of Eisele). Thus, Eisele teaches the claimed subject matter of claim 10.

V. Appellant has also argued that Eisele makes no teaching or suggestion of partitioning a memory or of the allocation of encrypted keys and other encrypted data between the partitions, as cited in claims 11-13 (see last line of page 16 through lines 1-2 of page 17 of appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

Figure 3, disk 7 is the one memory/storage device that contains magnetic disk 15, memory 9, and a processor 2, wherein the disk 7 is partitioning in a way so that, in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic

algorithms, secret codes etc. in such a way that they cannot be reproduced. To prevent unauthorized copying of programs or sections thereof, it is possible to store parts of these or the whole programs in the elements' processors. A program is particularly safe from unauthorized reproduction if one section is stored in the EDP-equipments' computer and the rest in processor 2 of any of the invented elements (see column 5, lines 20-30 of Eisele). Thus, Eisele has demonstrated the prima facies anticipation or obviousness of claims 11-13.

VI. Appellant has also argued that Eisele failed to show the address locations of the “first area” as cited in claims 13, 14, and 15 (see second paragraph, page 17 of appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

The rejection of claims 14 and 15 should be sustained for at least the same reasons given above in claims 11-13.

Figure 3, disk 7 is the one memory/storage device that contains magnetic disk 15, memory 9, and a processor 2, wherein the disk 7 is partitioning in a way so that, in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. in such a way that they cannot be reproduced. To prevent unauthorized copying of programs or sections thereof, it is possible to store parts of these or the whole programs in the elements' processors. A program is particularly safe from unauthorized reproduction if one section is stored in the EDP-equipments'

computer and the rest in processor 2 of any of the invented elements (see column 5, lines 20-30 of Eisele). Thus, Eisele has demonstrated the prima facies anticipation or obviousness of claims 14-15.

VII. As per claim 28, Appellant has argues with the same scope of invention as above in independent claim 1 and dependent claim 2 (see page 18-22 of appeal brief).

Again, Examiner respectfully disagrees with the appellant and still maintains that:

The rejection of claim 28 should be sustained for at least the same reasons given above in claims 1 and 2.

Eisele does teach the claimed subject matter of claim 28. It is clearly in Figure 2, 3, and 8, element 9 is a memory and column 5, lines 20-24 of Eisele stated that in order to use any of the elements as an encryption/decryption machine, it is necessary to load the element's memory units with one or more cryptographic algorithms, secret codes etc. (e.g., encryption key or master encryption key, etc..) in such a way that they cannot be reproduced. Figure 3 of Eisele clearly discloses element 9 is non-volatile memory and disk 7 is non-volatile magnetic memory. Therefore, Eisele precisely teaches the use of the two different memories to store encryption keys, i.e. a non-volatile memory to store the master encryption key and a non-volatile magnetic memory to store the encrypted encryption keys as recited by claim 28. Furthermore, claim 28 mentioned the reading of encryption keys and master encryption keys from two different memories, wherein the reading is similar to retrieving the keys from the storage area by comparing the PIN when user input from the

keyboard of the computer. The PIN then gets verified (retrieving the PIN that stored in the computer and comparing with the secret code input by user).

VIII. As for claims 27 and 30, Appellant's argument for these two claims is moot and should not be part of the argument, since their claim status were cancelled. (see page 23-24 of appeal brief).

Examiner believes that appellant has completely overlooked for the status of claims 27 and 30, which have been cancelled by the applicant on 9/15/2008 and that the amendment has been entered by the examiner on 10/1/2008..

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Thanhnga B. Truong/

Primary Examiner, Art Unit 2438

Conferees:

/Nasser Moazzami/

Supervisory Patent Examiner, Art Unit 2436

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438

.